110 年公務人員特種考試身心障礙人員考試試題

試 別：身心障礙人員考試
等 別：三等
考試類科：資訊處理
科 目：資通網路

一、㈠試說明網路路由器（ Router） 內部的組成元件？（15 分）
㈡試說明路由器造成資料傳送發生延遲或遺失的原因？（10 分）

擬答：

㈠網路路由器（ Router） 內部的組成元件

1. 連接埠口
每一埠口的實體層和鏈路層必須相同於其所連接之網路的通訊協定。

2. 轉送封包處理元件
目前 Internet 網路大多使用 IP 路由器，路由器拆解到封包的第三層協定標頭，即是 IP 封包標頭，再由標頭上 Destination Address (DA) 欄位利用路由表搜尋，決定轉送到哪一埠口。

3. 路由表
封包進入後依照目的位址，在路由表上搜尋下一個路徑（Next-hop）應該往哪一個埠口轉送。因此，建立路由表是一件重要的工作，一般路由表的建立方式有固定路由表（Fixed Routing Table）與動態路由表 (Dynamic Routing Table)。固定路由表一般應用在建構網路的拓樸圖，固定之後便不再變動，除非網路架構有所變動。大多應用於區域網路與子網路規畫上，因網路範圍不大甚少變動，以固定路由表即可。動態路由表由網路上之路由器隨時交換訊息建構而成，路由表的內容也隨時變動中。路由器之間交換訊息的內容和最佳路徑選擇演算法有不同的通訊協定規範，一般都使用 RIP（Routing Information Protocol）和 OSPF（Open Shortest Path First）協定。大多應用於網路範圍廣大，並可能網路架構隨時變更之網路，或不明網路架構如何之環境。

㈡

1. 由於路由器需要拆解封包，然後由標頭上 Destination Address 欄位利用路由表搜尋，決定轉送到哪一埠口，此一處理需要時間，因此造成延遲。
2. 若路由表設定錯誤，或是沒有交換到足夠的訊息內容，或是最佳路徑選擇演算法效能不佳，可能導致路由選擇錯誤，因而造成封包遺失。

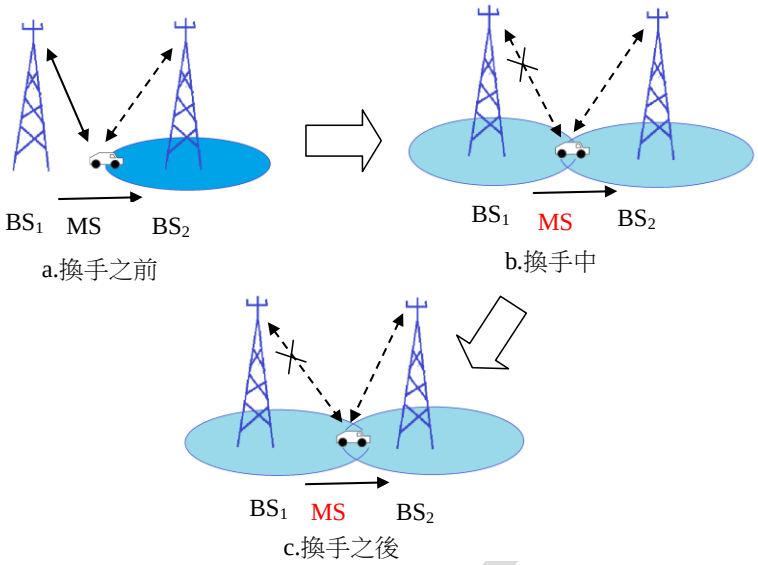
二、 在全球行動通訊系統（ GSM） 中， 換手（ handoff） 是經常發生的情形， 試說明當基地台（ BS） 決定要將行動使用者換手時會牽涉到的步驟（ 假設舊的基地台與新的基地台共用相同的行動服務交換中心 MSC） 。 （ 25 分）

【擬答】：

換手（handoff）運作時，當基地台發現行動電話的訊號越來越弱，它會詢問周圍的基地台，誰從該電話收到訊號的大小，然後基地台就會把所有權移給訊號強度最強的基地台，此一過程稱為交接。不過頻道指定是由 MTSO 完成，基地台只是中繼站。分為硬式換手與軟式換手。

㈠硬式換手（hard handoff）又叫做「先切斷後建立」（break before make），會先釋放與現有 BS 之間的無線電資源，然後才與新的 BS 建立連線。FDMA 與 TDMA 都是採用硬式換手。要謹慎選擇換手啟動的時機，以避免任何乒乓效應，且系統參數在換手時機的選擇上扮演重要的角

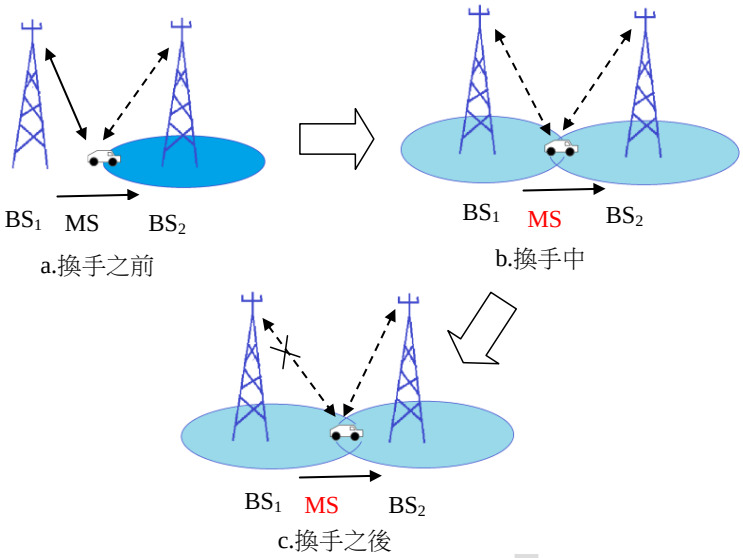
色。



Ref：Agrawal&Zeng

㈡軟式換手（soft handoff）

這種切換其工作原理是在不中斷與原基站的連通的情況下與新的基站連通，再與原基站斷開連接，即「先通後斷」。



Ref：Agrawal&Zeng

三、㈠試說明 TCP/IP 網路中， TCP 傳送端是如何察知自己和目的端之間的路徑發生壅塞情形？（10 分）

㈡試說明 TCP 對於壅塞情形的控制方法。 （ 15 分）

【擬答】：

㈠偵測發生壅塞

1. 基於遺失 (Loss-based)

傳統 TCP 將封包遺失視為壅塞的徵兆，以調整傳輸速率。判別當 TCP 區段遺失時，接收端採取何種重送機制，以執行對應策略，包括逾時重送(Retransmission Timeout)、快速重送(Fast Retransmission)。因為在網際網路平穩運行時，TCP 傳輸錯誤的比例很低，當區段遺失時，TCP 假設遺失是壅塞所造成。當接收端使用逾時重送(Retransmission Timeout)，表示接收端在逾時之前，未收到 3 個區段或送回的確認(ACK)遺失—壅塞嚴重的徵兆；當接收端使用快速重送(FastRetransmit)，表示接收端在逾時之前，已收到 3 個區段—壅塞輕微的

徵兆。

2. 基於與緩衝膨脹相關的延遲

如 TCP BBR（Bottleneck Bandwidth and Round-trip propagation time）是由 Google 設計，於 2016 年發布的壅塞演算法。該演算法使用網路最近出站資料分組當時的最大頻寬和往返時間來建立網路的顯式模型。封包傳輸的每個累積或選擇性確認用於生成記錄在封包傳輸過程和確認返回期間的時間內所傳送資料量的取樣率。

㈡ Internet 壅塞控制演算法

此演算法需要門檻（threshold）此一參數，初設為 64K，但是一旦發生逾時，則將門檻設成壅塞窗口的一半大小，再將壅塞窗口大小重設回一個最大區段。接著使用慢速啟動法來決定實際傳輸量，但在碰到門檻後，會改用線性成長方式探索最佳傳輸率。TCP 的壅塞控制方法主要可分為 Slow-start、Congestion-avoidance、Fast retransmission、Fast recovery 及 Timeout retransmission 五個階段；TCP 利用 ACK 偵測網路的狀況並提供可靠性的服務，在調整傳送端的傳送速度時，則以 Slow-start threshold 與 cwnd 的值來區分 Slow-start 或 Congestion-avoidance。

1. 當 cwnd 的值小於門檻-TCP 處於 slow-start phase

每收到一個 ACK，cwnd 的值*2，因為每經過一個 RTT 時間，cwnd 的值為上一個 RTT 時的 cwnd 值的 2 倍。此時的 cwnd 以 2 的指數的方式增加。

2. 當 cwnd 的值大於門檻-TCP 處於 congestion avoidance phase

每經過一個 RTT 時間，cwnd 的值才會增加一個 segment，以避免 cwnd 增加太快而導致封包遺失。此時的 cwnd 以線性的方式增加。

3. 傳送端收到 3 個 Duplicate ACK-TCP 會進行 Fast retransmit

此時首先要求接收端每收到一個失序的報文段後就立即發出重複確認，這樣做可以讓傳送端及早知道有報文段沒有到達接收方。傳送端只要一連收到三個重複確認會將封包視為遺失，不待 Timeout 便立即重送。接著將門檻的值設為 cwnd 的二分之一並將 cwnd 的值重設為 1，此時並非取消重傳計時器，而是在某些情況下可更早地重傳丟失的報文段。（TCP Tahoe 增加的功能）

4. Fast recovery 階段

用在 TCP Reno 協定中，在使用 Fast retransmit 重送遺失封包後，會將門檻以及 cwnd 的值都設為偵測到封包遺失時 cwnd 值的二分之一並進入 Fast recovery 階段，由於每收到一個 Duplicate ACK 也意味著有一個封包已經離開網路被接收端接收到了，因此如果允許的話，TCP Reno 還是可以使用 self-clocking 的機制繼續送出新的封包以提高 link 的使用率。如果封包遺失情形能夠在不需使用 Timeout retransmit 的情況下就將之回復，那麼 TCP Reno 在收到重送封包的 ACK 後就會直接進入 Congestion avoidance 階段，以加法增大方式使壅塞視窗緩慢地線性增大。

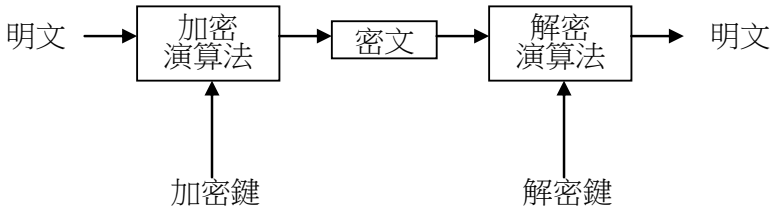
5. Timeout retransmission

當 RTO 計時器時間滿了之後，就會重新傳送新的封包。

四、在資料傳輸過程中， 確保資料的私密性、 完整性、 以及不可否認性非常重要， 其中密碼系統可確保資料的私密性、 雜湊函數可確保資料的完整性、以及數位簽章可確保資料的不可否認性。 試說明密碼系統、 雜湊函數、 以及數位簽章的運作過程。（25 分）

【擬答】：

㈠密碼系統中必須將明文根據加密演算法（encryption algorithm）獲得密文加以儲存或傳送，其中加密演算法需要輸入原始資料與加密鍵（encryption key），其中通常加密演算法是公開的，但是加密鍵則是只有需要知道的人才能知道。



㈡單向雜湊函數

文件訊息鑑別碼(MAC)可用來驗證文件訊息是否為約定好通訊的雙方所傳送，並可驗證文件訊息在傳遞過程中是否遭到篡改。單向雜湊函數 MAC 類型是利用一單向雜湊函數，配合一祕密金鑰所構成的訊息鑑別碼。此類的文件訊息鑑別碼機制也可讓使用者自行來決定要採用何種單向雜湊函數，在實作上相當便利也具有彈性。可任加一個區塊的文件訊息 M'到原文件訊息的後面其驗證的結果都會正確。以 MD5 單向雜湊函數演算法為例，若王五攔截到張三要傳給李四的文件訊息 M 及其訊息鑑別碼 H(K||M)，那麼王五根本不需要知道張三跟李四所協議的共同秘密金鑰 K 就可以任加一段訊息 M'至原訊息後面，且有辦法得到正確的訊息鑑別碼 H(K||M||M')。

1. 利用攔截到的 128 位元訊息鑑別碼 H(K||M)作為 MD5 中 A、B、C、D 四個暫存器的初始值。
2. 將添加訊息 M'分割成數個 512 位元的訊息區塊，再透過 MD5 演算法來做運算。
3. 最後得到的 128 位元輸出結果就等於 H(K||M||M')。

㈢數位簽章的運作方式如下圖所示，過程如下：

1. 產生 RSA 鍵對

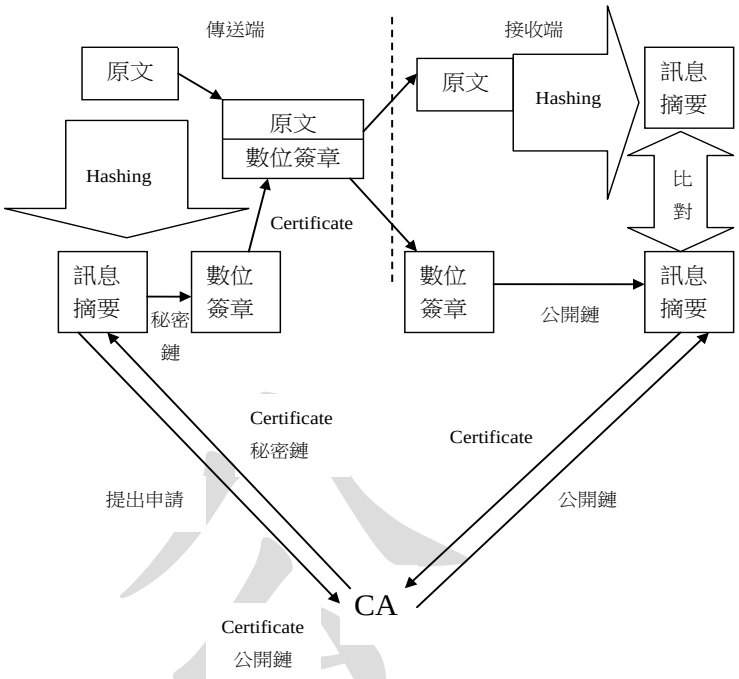
   在進行數位簽章處理之前，簽署者必須先產生自己的一對 RSA 鍵對，內容包括一把公開鍵及一把相對應的秘密鍵，並把其中公開鍵公佈給所有貿易伙伴知道，但卻私自隱密地保存秘密鍵，使不為外人所知。

2. 計算資料摘要並在加密後傳送

   在文件簽署之時，簽署者先把所要簽署的文件內容，經由一雜湊函數(Hash function)的運算，以得到與原文資料完全相關的資料摘要(Message digest)，之後再對這資料摘要以簽署者所獨自擁有的秘密鍵做加密運算，所得到的結果即為原文資料的數位簽章。簽署者並把這一數位簽章與原文資料一起傳送出去。

3. 接收端驗證

   驗證的一方在接到上述資料之後，首先把原文資料以相同的雜湊函數重新做運算，以得到一資料摘要。此外，驗證者也把所收到的數位簽章用簽署者所公佈的公開鍵做解密運算，而得到另一資料摘要。最後比對這兩個資料摘要是否相同，如果是，則表示所收到的資料確實是簽署者所簽署的文件資料。


傳送端
接收端
原文
原文
數位簽章
Hashing
原文
Hashing
訊息
摘要
比
對
Certificate
訊息
摘要
數位
簽章
秘密
鏈
數位
簽章
公開鏈
訊息
摘要
Certificate
秘密鏈
Certificate
提出申請
公開鏈
CA
Certificate
公開鏈